ADVANCES IN APPLIED MATHEMATICS 6, 350–372 (1985)

Ring Structures and the Discrete Fourier Transform

M. VULIS

Computer Science Department, City College of New York, New York, New York 10031

Since the pioneering work of J. W. Cooley and J. W. Tukey (*Math. Comp.* **19** (1965), 297–301), a great deal of effort has been devoted to developing efficient algorithms for computing finite Fourier transform. Among the new methods suggested over the past several years, methods depending on ring-theoretic structures have received special attention. This approach, originally suggested by C. Rader (*Proc. IEEE* **5**, **6** (1968), 1107–1108), was really developed by S. Winograd ("Arithmetic Complexity of Computations," CBMS-NSF Regional Conference Series in Applied Mathematics, 1980) into a powerful new algorithm. Winograd's real contribution was to realize that there are efficient algorithms to evaluate cyclic convolution. The purpose of this article is twofold: first, to make more explicit the interplay between ring-theoretic structures and the algorithms for the finite Fourier transform; second, to use this new insight to construct new algorithms for evaluating the finite Fourier transform on the groups $Z/(p^sZ) \oplus Z/(p^sZ) \oplus \cdots \oplus Z/(p^sZ)$.

0.0 INTRODUCTION AND EXAMPLES

0.1 *Fourier Transform: Definitions*

Let A be a finite Abelian group and let $\hat{A}$ be its dual or character group. Then, of course, A and $\hat{A}$ are isomorphic as abstract Abelian groups. Let $L^2(A)$ denote the set of complex valued functions $f(a)$ on the set A, with the norm of f, given by

$$\|f\|^2 = \sum_{a \in A} |f(a)|^2.$$

Let the pairing of A and $\hat{A}$ to the multiplicative group of complex numbers of absolute value 1, C_1^*, be denoted by $a * \hat{a} \to \langle a, \hat{a} \rangle \in C_1^*$. Then the Fourier transform F_A: $L^2(A) \to L^2(\hat{A})$ is defined for $f \in L^2(A)$, as

$$F_A(f)(\hat{a}) = \sum_{a \in A} \langle a, \hat{a} \rangle f(a).$$

0196-8858/85 $7.50

We will sometimes denote $F(f)$ as $\hat{f}$ and call f the *input* and $\hat{f}$ the *output* functions.

Consider the case when A is the cyclic group Z/nZ. Then A inherits the quotient ring structure from Z. Notice first that we can use it to identify Z/nZ and $(Z/\hat{n}Z)$ by defining

$$\langle K, L\rangle = e^{2\pi iKL/n}, \qquad K, L \in Z/nZ.$$

This pairing, although not functorial, will be fixed for the rest of this paper. Thus, if $e_j \in L^2(Z/nZ)$ is defined by

$$\begin{aligned} e_j(k) &= 1 \qquad \text{if } j = k \\ &= 0 \qquad \text{otherwise} \end{aligned}$$

then $e_0, e_1, \ldots, e_{n-1}$ is a basis in $L^2(Z/nZ)$, and if $f \in L^2(Z/nZ)$, then

$$f(k) = \sum_{k=0}^{n-1} f(k)e_k.$$

Relative to this basis,

$$\hat{f}(k) = \sum_{j=0}^{n-1} e^{2\pi ijk/n} f(j), \qquad k = 0, 1, \ldots, n-1.$$

We will denote the matrix $(e^{2\pi ijk/n})_{j,k=0,\ldots,n-1}$ by DFT$(n:1)$.

Of course, for $A = Z/n_1Z \oplus Z/n_2Z \oplus \cdots \oplus Z/n_sZ$, there are many ring structures on A and under judicious choice of ring structures we can use multiplication to define an isomorphism of A and $\hat{A}$. But even more is true; we will see that judicious choices of ring structure give rise to efficient algorithms for evaluating the finite Fourier transform F_A.

Winograd [W] used the ring structure on $Z/(p^sZ)$ to obtain an algorithm for evaluating DFT$(p^s:1)$. In [AFW] they similarly used the ring (field) structure on $Z/(pZ) \oplus Z/(pZ) \oplus \cdots \oplus Z/(pZ)$ to give an algorithm for evaluating DFT$(p:n)$. In this series of papers we will introduce a (local) ring structure on $Z/(p^sZ) \oplus Z/(p^sZ) \oplus \cdots \oplus Z/(p^sZ)$ to construct algorithms for evaluating DFT$(p^s:n)$.

Rather than dealing with this immediately on an abstract level, we will work out a few examples that illustrate how such algorithms can be constructed.

0.2. *One-Dimensional* DFT *on a Prime Number of Points*

EXAMPLE 1. $Z/7Z$. Since 7 is a prime, this ring is a finite field and so its multiplicative group $U(Z/7Z)$ is a cyclic group and it is easily verified that

3 is a generator of this group. We can list the elements of $Z/7Z$ in the following order: $\{0, 1, 3, 2 = 3^2, 6 = 3^3, 4 = 3^4, 5 = 3^5\}$. If $w = \exp(2\pi i/7)$ and $A(k)$, $k = 0, 1, \ldots, 6$ is in $L^2(Z/7Z)$, we have

$$\hat{A}(j) = \sum_{k=0}^{6} w^{jk} A(k). \tag{1}$$

Using the introduced ordering of the elements of $Z/7Z$, we write

$$\hat{A}(0) = A(0) + \sum_{k=0}^{5} A(3^k) \tag{2}$$

$$\hat{A}(3^{-j}) = A(0) + \sum_{k=0}^{5} w^{e^{k-j}} A(3^k). \tag{3}$$

Hence, there exist permutation matrices P and Q, such that

$$P \times \mathrm{DFT}(7;1) \times Q = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & X(1) & X(3) & X(2) & X(6) & X(4) & X(5) \\ 1 & X(5) & X(1) & X(3) & X(2) & X(6) & X(4) \\ 1 & X(4) & X(5) & X(1) & X(3) & X(2) & X(6) \\ 1 & X(6) & X(4) & X(5) & X(1) & X(3) & X(2) \\ 1 & X(2) & X(6) & X(4) & X(5) & X(1) & X(3) \\ 1 & X(3) & X(2) & X(6) & X(4) & X(5) & X(1) \end{Vmatrix},$$

where $X(k) = w^k$. The crucial thing to observe is that the 6×6 block in the lower right corner of the matrix F is a *circulant* matrix. We will denote this block by C7 and call it the *core* of the DFT(7 : 1). (Formally, a circulant square matrix is a K by K matrix M, such that $M(i, j) = M(i', j')$ if $i - i' \equiv j - j' \pmod{K}$. A more general definition will be given below.) A similar reordering that yields a large circulant core (which is based on the finite field structure) can always be carried out for DFT(p : 1), where p is any prime number.

Let us now consider Eqs. (2)–(3) from the computational point of view. It is clear that most of the computations in (3) are connected with the multiplication of an input 6-tuple by the matrix $C7$. Assume that we are to compute $Y = C7 \times X$, where X and Y are vectors of length 6. Generally, such an operation requires 36 multiplications and 30 additions. However, using a very special shape of the matrix $C7$, we can reduce the problem of the matrix multiplication to the problem of multiplication of two polynomi-

als as follows:

$$\text{Let } X(t) = \sum_{j=0}^{5} X(j)t^j,\ C7(t) = \sum_{j=0}^{5} W(3^j)t^j, \text{ and } Y(t) = \sum_{j=0}^{5} Y(j)t^j.$$

$$\text{Then } Y(t) = (X(t)C7(t)) \text{ modulo } (t^6 - 1). \tag{4}$$

There are at least two different algorithms which arise from these observations: First, we can view the operations performed in Eqs. (4) as the computation of the *convolution* of the input vector X with given vector $C7$. This will give rise to the *convolution* algorithm. Second, one can use more refined techniques connected with the polynomial multiplications, as done in the Winograd work [W]. This will produce so called Winograd Fourier transform algorithms. Both of these algorithms will utilize the circulant structure of $C7$, which is in turn caused by the underlying field structure.

We would like to complete this example with a discussion of a very special situation that arises when p is a Mercenne prime. If $p - 1$ is a power of 2, then the circulant core block will be a square matrix with side equal to power of 2. If so, Cooley–Tukey algorithm can be used to compute the cyclic convolution, producing quite an efficient algorithm. See [R] for more details.

0.3. *One-Dimensional* DFT *on a Power of a Prime Number of Points*

EXAMPLE 2. $Z/9Z$. Since 9 is not a prime number, but a power of prime number 3, $Z/9Z$ cannot be given a field structure, but can be given a structure of a local ring. Let $U = U(Z/9Z)$ be the unit group of $Z/9Z$. U consists of elements $1, 2, 4, 5, 7, 8$. It is easy to show that U is a cyclic group with 2 as a generator. Again let $A(j)$, $j = 0, 1, \ldots, 8$ be the input vector and $\hat{A}(j)$, $j = 0, 1, \ldots, 8$ be the output vector. Define

$$\begin{aligned}
B(0) &= A(0), & \hat{B}(0) &= \hat{A}(0),\\
B(1) &= A(3), & \hat{B}(1) &= \hat{A}(3),\\
B(2) &= A(3 \times 2), & \hat{B}(2) &= \hat{A}(3 \times 2^{-1}),\\
B(3) &= A(2^0), & \hat{B}(3) &= \hat{A}(2^0),\\
B(4) &= A(2^1), & \hat{B}(4) &= \hat{A}(2^{-1}),\\
B(5) &= A(2^2), & \hat{B}(5) &= \hat{A}(2^{-2}),\\
B(6) &= A(2^3), & \hat{B}(6) &= \hat{A}(2^{-3}),\\
B(7) &= A(2^4), & \hat{B}(7) &= \hat{A}(2^{-4}),\\
B(8) &= A(2^5), & \hat{B}(8) &= \hat{A}(2^{-5}).
\end{aligned}$$

Then $\hat{B} = F(9) \times B$, where, if $X(j) = \exp(2\pi i/9)$, $F(9)$ is given by the

matrix

1	1	1	1	1	1	1	1	1
1	1	1	$X(3)$	$X(6)$	$X(3)$	$X(6)$	$X(3)$	$X(6)$
1	1	1	$X(6)$	$X(3)$	$X(6)$	$X(3)$	$X(6)$	$X(3)$
1	$X(3)$	$X(6)$	$X(1)$	$X(2)$	$X(4)$	$X(8)$	$X(7)$	$X(5)$
1	$X(6)$	$X(3)$	$X(5)$	$X(1)$	$X(2)$	$X(4)$	$X(8)$	$X(7)$
1	$X(3)$	$X(6)$	$X(7)$	$X(5)$	$X(1)$	$X(2)$	$X(4)$	$X(8)$
1	$X(6)$	$X(3)$	$X(8)$	$X(7)$	$X(5)$	$X(1)$	$X(2)$	$X(4)$
1	$X(3)$	$X(6)$	$X(4)$	$X(8)$	$X(7)$	$X(5)$	$X(1)$	$X(2)$
1	$X(6)$	$X(3)$	$X(2)$	$X(4)$	$X(8)$	$X(7)$	$X(5)$	$X(1)$

Let us examine this matrix. The 6 by 6 block in the lower right corner which we denote by $C9$ is called the *core* of the DFT(9 : 1) and is a circulant matrix. Similarly to the prime case above, multiplication by C9 can be performed by using Winograd's convolution technique. The two rectangular matrices allow us to illustrate new effects. Each of them is obtained by repetitions of the same 2 by 2 subblock. We immediately observe that

(1) to multiply an input vector by either of these rectangular matrices it suffices to perform a few additions and multiply an input vector of length 2 by the 2 by 2 subblock;

(2) this subblock is nothing else than the *core* matrix $C3$ appearing in DFT(3 : 1). This result will be explained later and connected to the canonical epimorphism $Z/9Z \to Z/3Z$.

0.4. *Multi-dimensional* DFT *on a Prime Number of Points*

The following example is taken from the work by Auslander, Feig, and Winograd [AFW].

EXAMPLE 3. $Z/3Z \oplus Z/3Z$. Consider $A = Z/3Z \oplus Z/3Z$ and the finite Fourier transform on this group denoted by DFT(3 : 2), where $Z/3Z$ is identified with $Z(3Z)^{\wedge}$ as before and so A is identified with $\hat{A}$. Thus the input data $A(j, k)$, where $j, k = 0, 1, 2$ is indexed by two variables. For the purpose of this example we will give A a ring structure which is different from the product ring structure.

Let $f(u)$ be a polynomial which is irreducible over $Z/3Z$. Then it is well known that $(Z/3Z)[u]/(f(u))$ is a finite field $F(9)$ of 9 elements. Its additive group is A. We will choose $f(u) = u^2 + 1$ which is an irreducible polynomial over $Z/3Z$. Then (and similarly for any other primes p which are congruent to 3 modulo 4) there is an alternative way of describing the obtained ring structure, which we will adapt for this example.

Let $Z[i] = \{a + bi/a, b \in Z\}$ denote the ring of Gaussian integers and let (3) be the ideal generated by 3 in $Z[i]$. Then (3) is a prime ideal and so $Z[i]/(3)$ is a field $F(9)$ where the additive group is isomorphic to $Z/3Z \oplus Z/3Z$. In $F(9)$ let U denote the group of units. Then U is cyclic and $1 + i = (1, 1) \in Z/3Z \oplus Z/3Z$ is a generator. Let $B(0) = A(0)$, $B(k) = A((1 + i)^{k-1})$ for $k = 1, 2, \ldots, 8$. Similarly, let us rearrange the output $\hat{A}$ by setting $\hat{B}(0) = \hat{A}(0)$ and $\hat{B}(b) = \hat{A}((1 + i)^{1-k})$. If $\hat{B} = F(3, 2) \times B$ and $X(j) = \exp(2\pi ij/3)$, then DFT(3 : 2) is the matrix

$$\left\|\begin{array}{c|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & X(1) & X(1) & 1 & X(1) & X(2) & X(2) & 1 & X(2) \\ 1 & X(2) & X(1) & X(1) & 1 & X(1) & X(2) & X(2) & 1 \\ 1 & 1 & X(2) & X(1) & X(1) & 1 & X(1) & X(2) & X(2) \\ 1 & X(2) & 1 & X(2) & X(1) & X(1) & 1 & X(1) & X(2) \\ 1 & X(2) & X(2) & 1 & X(2) & X(1) & X(1) & 1 & X(1) \\ 1 & X(1) & X(2) & X(2) & 1 & X(2) & X(1) & X(1) & 1 \\ 1 & 1 & X(1) & X(2) & X(2) & 1 & X(2) & X(1) & X(1) \\ 1 & X(1) & 1 & X(1) & X(2) & X(2) & 1 & X(2) & X(1) \end{array}\right\|.$$

We could evaluate $\hat{B}$ by convolution techniques, but here a substantially more powerful approach can be used. Let E be the 8 by 8 matrix all of whose entries are equal to 1. Then, if $C(3 : 2)$ is the 8 by 8 circulant subblock in the bottom right corner of $F(3 : 2)$, we can write $C(3 : 2) = E + M1 \times M2$, where

$$M1 = \left\|\begin{array}{cccccccc} X(1) & 0 & 0 & 0 & X(2) & 0 & 0 & 0 \\ 0 & X(1) & 0 & 0 & 0 & X(2) & 0 & 0 \\ 0 & 0 & X(1) & 0 & 0 & 0 & X(2) & 0 \\ 0 & 0 & 0 & X(1) & 0 & 0 & 0 & X(2) \\ X(2) & 0 & 0 & 0 & X(1) & 0 & 0 & 0 \\ 0 & X(2) & 0 & 0 & 0 & X(1) & 0 & 0 \\ 0 & 0 & X(2) & 0 & 0 & 0 & X(1) & 0 \\ 0 & 0 & 0 & X(2) & 0 & 0 & 0 & X(1) \end{array}\right\|$$

$$M2 = \left\|\begin{array}{cccccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right\|$$

This decomposition allows one to save substantially on the number of arithmetic operations which are required to effect the transform. Observe next that $M1$ can be permuted into a block-diagonal matrix with four 2 by 2 blocks on the diagonal, each of them being

$$C3 = \begin{Vmatrix} X(1) & X(2) \\ X(2) & X(1) \end{Vmatrix}.$$

0.5. *Ring Structures and Circulant Blocks*

We will give a brief discussion of how the ring structures on the group $G = Z/mZ \oplus Z/mZ \oplus \cdots \oplus Z/mZ$ can give rise to circulant blocks in the matrix representing Fourier transform DFT$(m: n)$.

If $k = (k_0, \ldots, k_{n-1})$ and $j = (j_0, \ldots, j_{n-1})$, then

$$\hat{A}(k) = \sum_j w^{\langle k, j \rangle} A(j), \tag{5}$$

where $w = \exp(2\pi i/m)$ and $\langle k, j \rangle = \sum_{\alpha=0}^{n-1} k_\alpha j_\alpha$. Let X and Y be subsets of G. Consider the "partial" transform, defined as follows: For $k \in X$, define

$$B(k) = \sum_{j \in Y} w^{\langle k, j \rangle} A(j). \tag{6}$$

If the transform (5) is written in matrix form by ordering k and j lexicographically, then the partial transform corresponds to a submatrix of DFT$(m: n)$. We may ask: "When is this submatrix circulant?"

Let us consider first the case where $G = Z/mZ$. Then $\langle k, j \rangle = kj$. Let x be an element in the unit group. Then there exist an integer $r > 0$, such that $x^r = 1$ and so $x^{-1} = x^{r-1}$. Now for some $a, b \in G$ define

$$X = \{a, ax, \ldots, ax^{r-1}\} \qquad \text{and} \qquad Y = \{b, bx^{-1}, \ldots, bx^{1-r}\}.$$

(Of course, the elements in the brackets need not be different.) By (6),

$$B(ax^k) = \sum_{j=0}^{r-1} w^{(abx^{(k-j)})} A(bx^{-j}). \tag{7}$$

Then the corresponding square r by r matrix M, where $M(k, j) = w^{(abx^{(k-j)})}$, will be circulant.

We will now consider the general case, where $G = Z/mZ \oplus \cdots \oplus Z/mZ$. Let Φ: $G \to Z/mZ$ be defined by $\Phi(k_0, \ldots, k_{n-1}) = k_0$. Assume that G has been given a ring structure R (the additive group of R is G) and there exists a mapping J: $G \to G$ such that for any $a, b \in G$

$$\langle J(a), b \rangle = \Phi(ab). \tag{8}$$

Now let $U(R)$ be the unit group of R and let $x \in U(R)$. For $a, b \in G$ define $X = \{a, ax, \ldots, ax^{r-1}\}$ and $Y = \{J(b), J(bx^{-1}), \ldots, J(bx^{1-r})\}$, where r is the order of x. Then the partial transform relative to the sets X and Y will produce a matrix, which is not necessarily circulant. The main

difficulty here is the fact that the elements, listed in the definition of X and Y, might not be distinct. That will be the case if for some $r' < r$, $ar' = a$, or $br' = b$. In order to handle this situation, we will somewhat generalize the picture.

Notation. By $E_{K,L}$ we will mean the K by L matrix with all entries equal to 1.

DEFINITION. We say that a K by L rectangular matrix M is circulant, if $M(i, j) = M(i', j')$ when $i - i' \equiv j - j' \pmod{K}$ or $i - i' \equiv j - j' \pmod{L}$.

Remark. The last conditions are clearly equivalent to saying that $i - i' \equiv j - j' \pmod{\mathrm{GCD}(K, L)}$, where $\mathrm{GCD}(K, L)$ is the greatest common divisor of K and L.

LEMMA 1. *Any rectangular circulant matrix M can be written as $E_{(K/Q, L/Q)} \otimes N$, where $Q = \mathrm{GCD}(K, L)$ and N is the square Q by Q major minor of M.*

Proof. Let $E = E_{(K/Q, L/Q)}$. Any $i = 0, \ldots K - 1$ can be uniquely written as $i_0 + i_1 Q$, where $i_1 = 0, \ldots, K/Q - 1$ and $i_0 = 0, 1, \ldots, Q - 1$. Similarly, any $j = 0, \ldots, L - 1$ can be uniquely written as $j_0 + j_1 Q$, where $i_1 = 0, \ldots, L/Q - 1$ and $i_0 = 0, 1, \ldots, Q - 1$. Therefore, $M(i, j) = M(i_0 + i_1 Q, j_0 + j_1 Q) = M(i_0, j_0) = M(i_0, j_0) E(i_1, j_1)$, which complies with the definition of the tensor product. □

Let $x \in U(R)$. Let O_1 and O_2 be orbits in R under the (multiplicative) action of x. Let O_1 and O_2 contain K and L elements, respectively, $O_1 = \{a, ax, \ldots, ax^{K-1}\}$ and $O_2 = \{a, ax, \ldots, ax^{L-1}\}$. Note, that we can also write $O_2 = \{b, bx^{-1} = bx^{L-1}, \ldots, bx^{1-L} = bx\}$.

We claim that the partial transform corresponding to the sets $J(O_2)$ and O_1 is given by a circulant matrix. Indeed, the matrix of this partial transform is

$$\left\| {}_W\langle J(bx^{-i}), ax^j \rangle \right\|_{\substack{j=0,\ldots,K-1 \\ i=0,\ldots,L-1}} = \left\| {}_W\Phi(abx^{j-i}) \right\|_{\substack{j=0,\ldots,K-1 \\ i=0,\ldots,L-1}}. \tag{9}$$

In order to comply with the definition, we have to show that $\Phi(abx^{j'-i'}) = \Phi(abx^{j-i})$ if $j' - i' \equiv j - i \pmod{K}$ or $j' - i' \equiv j - i \pmod{L}$. Assume, for example, that $j' - i' = j - i + \alpha K$ for some integer α. Then $\Phi(abx^{j'-i'}) = \Phi(abx^{j-i+\alpha K}) = \Phi(ax^{\alpha K} bx^{j-i}) = \Phi(abx^{j-i})$, since $ax^{\alpha K} = a$ and the statement on circulant matrices follows.

We can now consider the whole transform. Let x be as before and let $R = U_t O_t$, where O_t are disjoint (multiplicative) orbits. Then for any t, t', the partial transform corresponding to $(J(O_{t'}), O_t)$ is given by a circulant matrix, and, therefore,

THEOREM 2. *Let* $G = Z/mZ \oplus Z/mZ \oplus \cdots \oplus Z/mZ$ *and* Φ *and* J *be as above. Then the matrix of the Fourier transform can be permuted into a block-structured matrix which contains circulant blocks, corresponding to disjoint multiplicative orbits. This permutation can be performed by ordering all the elements of the ring by multiplicative orbits under the action of a selected element of the unit group.*

Remark. It is now clear that (generally) we will get most advantage in the situation where large orbits (and, hence, large circulant blocks) are present.

0.6. *An Example for the Composite Case*

EXAMPLE 4. $Z/6Z \oplus Z/6Z$. We would like to present one last example, which involves a very large circulant block. We find this example deserving attention, even if it does not give rise to a general algorithm and will not be fully covered by the subsequent theory.

Let us consider the ring which is the direct sum of finite fields of four elements, $F(4)$ and that of nine elements, $F(9)$. We denote it $R(36)$.

The additive group of $F(4)$ is $Z/2Z \oplus Z/2Z$ and the additive group of $F(9)$ is $Z/3Z \oplus Z/3Z$. Therefore the additive group of $R(36)$ is isomorphic to $Z/6Z \oplus Z/6Z$. Multiplicatively, the unit groups of $F(4)$ and $F(9)$, $U(F(4))$ and $U(F(9))$, are cyclic groups of orders 3 and 8 correspondingly. Since these numbers are relatively prime, $U(R(36)) = U$ is a cyclic group of order 24.

There is an alternative way of describing $R(36)$. We can view it as $Z(6)[u]/(u^2 - u - 1)$, where $Z(6)$ is the ring of integers modulo 6. Indeed, $u^2 - u - 1$ is irreducible both over $F(2)$ and $F(3)$, $Z(6) = F(2) \oplus F(3)$, and

$$F(6)[u]/(u^2 - u - 1) \approx F(2)[u]/(u^2 - u - 1) \oplus F(3)[u]/(u^2 - u - 1).$$

In this representation it is not hard to see that u generates the unit group. Indeed,

$u^0 = 1$	$u^6 = 5 + 2u$	$u^{12} = 5$	$u^{18} = 1 + 4u$
$u^1 = u$	$u^7 = 2 + u$	$u^{13} = 5u$	$u^{19} = 4 + 5u$
$u^2 = 1 + u$	$u^8 = 1 + 3u$	$u^{14} = 5 + 5u$	$u^{20} = 5 + 3u$
$u^3 = 1 + 2u$	$u^9 = 3 + 4u$	$u^{15} = 5 + 4u$	$u^{21} = 3 + 2u$
$u^4 = 2 + 3u$	$u^{10} = 4 + u$	$u^{16} = 4 + 3u$	$u^{22} = 2 + 5u$
$u^5 = 3 + 5u$	$u^{11} = 1 + 5u$	$u^{17} = 3 + u$	$u^{23} = 5 + u.$

It is not hard to show that we can satisfy Eq. (8) by choosing identity mapping J. Therefore, by Theorem 2, the partial transform, corresponding to (U, U) is given by a circulant 24 by 24 matrix. If we denote by $\mathrm{cyc}(a(0), \ldots, a(k-1))$ the circulant matrix with first row equal to $(a(0), \ldots, a(k-1))$, then this partial transform is given by

$$\begin{aligned}\mathrm{cyc}(&X(1), X(0), X(1), X(1), X(2), X(3), X(5), X(2),\\ &X(1), X(3), X(4), X(1), X(5), X(0), X(5), X(5)\\ &X(4), X(3), X(1), X(4), X(5), X(3), X(2), X(5)),\end{aligned}$$

where $X(t) = \exp(2\pi it/6)$.

The other partial transforms will involve the remaining shorter orbits. Under the multiplicative action of u, they are

$$\begin{aligned}O(1) &= \{0\}\\ O(2) &= \{2, 2u, 2+2u, 2+4u, 4, 4u, 4+4u, 4+2u\}\\ O(3) &= \{3, 3u, 3+3u\}.\end{aligned}$$

Thus, if we reorder the input and output data by first listing the entries indexed by $O(1)$, then $O(2)$, $O(3)$, and U, the matrix of DFT(6 : 2) will be permuted into a matrix of the following block shape:

	$O(1)$	$O(2)$				$O(3)$		$O(24)$										
$O(1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$O(2)$	1					1	1											8
	1					1	1											
	1					1	1											
	1					1	1											
$O(3)$	1	1	1	1	1													3
	1	1	1	1	1													
U	1																	24
	1																	
	1																	
	1																	
	1																	
	1																	
	1																	
	1																	
	1																	
	1																	
	1	8				3		24										

Here all the highlighted blocks are circulant; the numbers to the right and below the figure denote the size. Some of the blocks (ones filled with 1 on the figure) contain only ones. As mentioned above, all the rectangular blocks contain repeated smaller square circulant blocks.

It is beyond the purpose of this paper to go into detailed structure of the blocks; we will only say that a special-purpose algorithm computing DFT(6 : 2) can be constructed on the basis of observations we have just made.

Remark. There is one more important observation to be made from this example: the orbits (and so the partial transforms) corresponding to the zero divisors of the ring are generally more complicated than the unit group and special care should be exercised with them.

I. General Remarks on Commutative Local Rings

This section will be devoted to the development of the algebraic results that we will need for the rest of the paper. To simplify language, we will use "ring" and "group" to denote finite commutative ring with 1 and finite Abelian group. We will reserve "p" to denote an odd prime integer and $q = p^s$, where s is a fixed integer number. Further, we will use notation $Z(m)$ to denote the ring of integers modulo m as opposed to the group of integers modulo m, Z/mX. $F(n)$ will denote the finite field of n elements.

We will begin with a brief review of some well-known, if not quite standard, algebra.

Definition. A (commutative) ring R is said to be a *Local ring* if R possesses unique maximal ideal.

Examples. The only ideal in a field is the zero ideal. Thus the zero ideal of a field is the unique maximal ideal, and hence any field is a local ring.

Clearly, $Z(q)$ is a local ring with the principal ideal (p) as the maximal ideal. Of course, $(p^2), (p^3), \ldots, (p^{s-1}), (0)$ are also ideals in $Z(q)$.

Definition. Let N be the maximal ideal of a local ring R. Then R/N is a field, called the *Residue field* of the local ring R. Since R possesses only one maximal ideal, its residue field is unique. The quotient map $R \to R/N$ is called the *Residue map* of the local ring R.

We recall that the set of elements U of R such that $r \in U$ if and only if there exists $r' \in R$ such that $rr' = 1$ is easily seen to be a group under multiplication and is called the unit group of R. When R is a local ring with unique maximal ideal N, $U = R - N$ where minus denotes the set-theoretic difference. This is because if $r \in R - N$, the ideal generated by r, (r), is not

in N and so must be equal to R. Hence, there exists r', $rr' = 1$ and so $r \in U$.

DEFINITION. Let R be a ring and I an ideal in R. We call I nilpotent if there exist an integer k, such that for any $r_1, \ldots, r_k \in I$ $r_1 \ldots r_k = 0$.

Remark. If I is a nilpotent ideal in ring R, then $1 + I = \{1 + i/i \in I\}$ is a (multiplicative) subgroup of the unit group $U(R)$. (Cf. [AM].)

LEMMA 3. *Let N be a maximal ideal of R that is nilpotent. Then R is a local ring.*

Proof. The lemma is equivalent to the statement that N is the unique maximal ideal of R. Notice if $a \in R$, such that a^{-1} exists, then the ideal generated by a, (a), is equal to R. Hence no proper ideal can contain an invertible element of R. We will now show that our hypothesis guarantees that N contains all the non-invertible elements of R.

Let a be non-invertible element of R and not be in N. Then, since N is a maximal ideal, $(a) + N = R$. Hence there exist $b \in (a)$ and $n \in N$, such that $b + n = 1$. Since n is a nilpotent element, there exists a positive integer k, such that $n^k = 0$. Hence

$$1 = 1^k = b^k + \cdots + kbn^{k-1} + 0 = b(b^{k-1} + \cdots + kn^{k-1}),$$

and so b is invertible. Hence $(a) = R$ and hence there exists $r \in R$, such that $ar = 1$, and a is invertible, which is a contradiction. □

We next review a few basic facts about polynomial extensions of rings.

(1) Let R be a ring, let I be an ideal in R and let $R[u]$ be the polynomial ring over R, where u is an undeterminate over R. Clearly, then $I[u]$ is a subring of $R[u]$ and $R[u]/I[u]$ is isomorphic to $(R/I)[u]$.

(2) Let $f(u) \in R[u]$. Let

$$I' = \{g(u) \in I[u] | g(u) \text{ is divisible by } f(u)\}.$$

Then I' is an ideal in $I[u]$. Let $I[u]/\langle f(u)\rangle \approx I[u]/I'$. Then

$$(R[u]/\langle f(u)\rangle)/(I[u]/\langle f(u)\rangle) \approx (R/I)[u]/\langle f'[u]\rangle$$

where $f'[u]$ is the image of $f(u)$ in $R/I[u]$.

(3) Let N be a nilpotent ideal in R. Then $N[u]$ is a nilpotent ideal in $R[u]$.

We would like to extend the following construction to local rings. Let F be a field, and f' an irreducible polynomial over F. Then $F[u]/\langle f'(u)\rangle$ is a finite field. The problem is that it does not make sense to talk about

irreducible polynomials over a local ring. To overcome this difficulty, we introduce the following.

DEFINITION. Let R be a local ring with maximal ideal N and residue field F. We extend the residue mapping $\pi\colon R \to F$ to a homomorphism $\pi[u]\colon R[u] \to F[u]$ by letting $(\pi[u])(r) = \pi(r)$ for $r \in R$. We say that $f(u) \in F[u]$ is a *locally irreducible polynomial* if $f' = (\pi[u])(f) \in F[u]$ is an irreducible polynomial over F and the degree of f' over F is equal to the degree of f over R.

Consider now the following commutative diagram, where $f \in R[u]$ and f is locally irreducible.

$$\begin{array}{ccccccccc}
1 & \to & N & \to & R & \to & F & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & N[u] & \to & R[u] & \to & F[u] & \to & 1\cdot \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & N[u]/\langle f(u)\rangle & \to & R[u]/\langle f(u)\rangle & \to & F[u]/\langle f'(u)\rangle & \to & 1
\end{array}$$

LEMMA 4. *$R_1 = R[u]/\langle f(u)\rangle$ is a local ring with maximal ideal $N_1 = N[u]/\langle f(u)\rangle$ and residue field $F_1 = F[u]/\langle f(u)\rangle$.*

Proof. Because $R_1/N_1 = R/N[u]/(f'(u))$ and f' is, by hypothesis, irreducible in $F[u]$, $F = R/N$, we see that R_1/N_1 is a field so N_1 is a maximal ideal in R_1. All that remains is to verify that N_1 is nilpotent, so we can apply lemma 1. We present N_1 as $N \oplus uN \oplus \cdots \oplus u^{n-1}N$, where n is the degree of f. Since N is nilpotent, N_1 is also nilpotent. □

II. BACK TO THE BASIC PROBLEM

Consider the group $Z/qZ \oplus \cdots Z/qZ$, where $q = p^s$. We wish to supply this group with a local ring structure satisfying the hypothesis of Theorem 2. We will now proceed with this construction.

Clearly, $Z(q)$ is a local ring with residue field $F(p) = Z(p)$. It is well known that for any $n \geq 1$ there is an irreducible polynomial f_n' of degree n over $F(p)$. Since $\pi[u]\colon Z(q)[u] \to Z(p)[u]$ is a surjection, there exists $f_n \in Z(q)[u]$ which is locally irreducible; $\pi[u](f_n) = f'$. Then $Z(q)[u]/(f_n[u])$ is a local ring with $Z(p)[u]/(f_n'[u])$ as residue field. Clearly the additive structure of $Z(q)[u]/(f_n[u])$ is isomorphic to $Z/qZ \oplus Z/qZ \oplus \cdots \oplus Z/qZ$.

To simplify the notation, let

$$Z(q:n) = Z(q)[u]/(f_n[u])$$
$$Z(p:n) = Z(p)[u]/(f_n'[u]).$$

Here $Z(p:n)$ is the finite field with p^n elements which we also denote by $F(p^n)$.

Conventions. We will always be working with the above presentations of $Z(p:n)$ and $Z(q:n)$ and consider their elements as polynomials modulo $f_n'(u)$ and $f_n(u)$, respectively. We will always use u to denote the coset of u and will often write $Z(q:n) = Z(q) \oplus uZ(q) \oplus \cdots \oplus u^{n-1}Z(q)$.

Denote the group of units $Z(q:n)$ by $U(q:n)$. Since $pZ(q:n)$ is the unique maximal ideal of $Z(q:n)$, $U(q:n)$ consists of all polynomials $a = a_0 + a_1u + \cdots + a_{n-1}u^{n-1} \in Z(q:n)$, such that a_j is not divisible by p for some $0 \le j < n$. Consider $a \in Z(q:n)$, $a \neq 0$, $a = a_0 + \cdots + a_{n-1}u^{n-1}$. Let $a_i = p^{r(i)}a_i'$ for $i = 0, \ldots n-1$ with a_i' not divisible by p. Let k be the minimum of $r(0), \ldots, r(n-1)$. Then $a = p^k v$, where $v \in U(q:n)$, since at least one of the coefficients of v is not divisible by p. Hence the orbits of $U(q:n)$ multiplicatively acting on $Z(q:n)$ are $U(q:n)$, $pU(q:n)$, $p^{s-1}U(q:n)$, $\{0\} = p^sU(q:n)$. It is also clear that (p) contains exactly $p^{(s-1)n}$ elements. This implies that $U(q:n)$ contains $p^{(s-1)n}(p^n - 1) = p^{sn} - p^{(s-1)n}$ elements.

If $a = a_0 + a_1u^1 + \cdots a_{n-1}u^{n-1} \in Z(q:n)$ we define $\Phi(a) = a_0 \in Z(q)$. Of course, Φ is an additive epimorphism and the following diagram is commutative:

$$\begin{array}{ccc} Z(q:n) & \xrightarrow{\pi} & Z(p:n) \\ \Phi \downarrow & & \downarrow \Phi \\ Z(q) & \xrightarrow{\pi} & Z(p) \end{array} .$$

III. Conjugation Automorphism

We will now proceed to the definition of the automorphism J, satisfying the hypothesis of Theorem 2.

We will start this construction with some general observations.

Definition. Let R be any ring, such that its additive group is $G \approx Z/mZ \oplus \cdots \oplus Z/mZ$. Let Θ: $G \to Z/mZ$ be a group homomorphism. We say that a group endomorphism J: $G \to G$ is a conjunction, associated to Θ, if

$$\langle J(a), b\rangle = \Theta(ab), \qquad \text{for any } a, b \in R. \tag{10}$$

In the constructions below we will view elements of R as n-tuples $(a_0, \ldots, a_{n-1})$. Let $e^i \in R$ be the element $(0, 0, \ldots, 1, 0, 0)$, where 1 occupies the ith position.

LEMMA 5. *For a given Θ, there is at most one associated conjugation.*

Proof. Assume that (10) holds for both J_1 and J_2. Then for any $a, b \in R$, $\langle J_1(a), b\rangle - \langle J_2(a), b\rangle = \langle K(a), b\rangle = 0$, where $K = J_1 - J_2$ is an endomorphism of G. We will show that K is the zero mapping; indeed assume that for some $a \in R$, $K(a) = (c_0, c_1, \ldots, c_{n-1})$ and for some k, c_k is not equal to 0. Then $\langle K(a), e^k\rangle \neq 0$ and we obtain a contradiction. Therefore, $J_2 = J$. □

We next consider the question of existence. The multiplication in R can be defined by the table of structure constants as follows:

$$\text{Let } e^i e^j = \sum_{k=0}^{n-1} C_k^{ij} e^k. \quad \text{Then for any } a, b \in R,\ ab = \sum C_k^{ij} a_i b_j e^k.$$

We term C the array of *Structure constants*.

All the entries of C are elements of Z/mZ. We observe that different properties of R can be described on the language of structure constants; for example, R is commutative if and only if $C_k^{ij} = C_k^{ji}$ for any $i, j = 0, \ldots, n - 1$.

Similarly, Θ can be described by its action on the "basis" $\{e^i\}$. Let $\Theta(e^k) = \Theta^k \in Z/mZ$ for $k = 0, \ldots, n - 1$. Then for any $a \in R$, $a = \sum_{k=0}^{n-1} a_k e^k$, $\Theta(a) = \sum_k \Theta^k a_k$. Hence, for any $a, b \in R$, $\Theta(ab) = \sum_i \sum_j \sum_k C_k^{ij} \Theta^k a_i b_j$. We now define $J(a) = \sum_i \sum_j \sum_k C_k^{ij} \Theta^k a_i e^j$. It is easy to see that (10) is satisfied and J is, therefore, the conjugation of R, associated to Θ.

We have thus shown that any finite ring R, whose additive group is $Z/mZ \oplus \cdots \oplus Z/mZ$ possesses a unique conjugation. However, in view of Theorem 2, we would like to be able to consider this conjugation as a permutation or J to be bijective. In the general case J need not to be bijection; an obvious example of this would be the zero ring. where all the structure constants are defined to be zero. The next theorem will show that J is indeed bijective when $R = Z(q: n)$ and $\Theta = \Phi$.

THEOREM 6. *There exists a unique automorphism J of the additive group of the ring $Z(q: n)$, such that the following equation holds:*

$$\langle J(a), b\rangle = \Phi(ab), \qquad \text{for any } a, b \in Z(q: n). \tag{11}$$

COROLLARY. *The finite Fourier transform matrix of the group $Z/qZ \oplus \cdots \oplus Z/qZ$ can be decomposed into circulant blocks.*

Proof. The uniqueness follows immediately from Lemma 5. To show the existence, we will provide a description of J different from the one above. Let C be the companion matrix of the polynomial f over $Z(q)$. Then the

mapping $\sum_{i=0}^{n-1} a_i u^i \to \sum_{i=0}^{n-1} a_i C^i = a(C)$ is a matrix representation of $Z(q:n)$ in the ring of all n by n matrices over $Z(q)$. Notice that the first column of $a(C)$ is $(a_0, a_1, \ldots, a_{n-1})^t$, hence $\sum_{i=0}^{n-1} a_i u^i = \sum_{i=0}^{n-1} (a(C))_{i,0} u^i$. (Here we use the subscripts 0 through $n-1$ to denote the entries of a matrix.) Define $J(a) = \sum_{i=0}^{n-1} (a(C))_{0,i} u^i$.

Clearly, J is an additive endomorphism of $Z(q:n)$. J also satisfies Eq. (11), because

$$\langle J(a), b\rangle = \sum_{i=0}^{n-1} (J(a))_i b_i = \sum_{i=0}^{n-1} (a(C))_{0,i} (b(C))_{i,0}$$

$$= (a(C)b(C))_{0,0} = ((ab)(C))_{0,0} = \Phi(ab).$$

To complete the proof we have to show that J is bijective. Let us assume that there exists $a \neq 0$, $a \in \mathrm{Ker}(J)$. Then the first row of the matrix $a(C)$ must contain only zeroes, and, so, $a(C)$ is not an invertible matrix and hence a is not an invertible element in $Z(q:n)$. Further, a is not one of the elements $p, p^2, p^3, \ldots, p^{s-1}$, since $p^k(C)$ contains a nonzero leading entry. Since, for any $a \neq 0$, $a \in Z(q:n)$ there always exist $k > 0$ and an element $g \in Z(q:n)$ such that $ag = p^k$ for some integer k, we have

$$(p^k(C))_{0,0} = \sum_{i=0}^{n-1} (a(C))_{0,i} (g(C))_{i,0} = 0,$$

which is not possible. This proves that J is an injection; that J is a surjection follows from the finiteness of $Z(q:n)$. □

Remark. For $n = 1$, J becomes the identity map.

We now prove a few elementary properties of J.

LEMMA 7. (1) $\Phi(a) = \Phi(J(a))$, *for any* $a \in Z(q:n)$.

(2) $J((p^k)) = (p^k)$, *for every* k.

(3) *If we specify the basis* $(1, u, u^2, \ldots, u^{n-1})$, *then* J *is given by a symmetric block-diagonal matrix with two blocks: the first one is the* 1 *by* 1 *identity matrix and the other is an* $(n-1)$ *by* $(n-1)$ *matrix.*

Proof. Statement (1) immediately follows from the definition of J. Now $a \in (p^{s-1})$ is and only if $pa = 0$. But then $J(pa) = 0$ because J is an additive homomorphism. Statement (2) will follow by a simple induction. To prove (3), we will consider J as a linear operator. Let J also denote the matrix of J in the basis $(1, u, u^2, \ldots)$. By definition of J $\langle J(u^j), u^k\rangle = \langle u^j, J(u^k)\rangle$ for any j and k, and, therefore J is symmetric. Finally,

$J = \langle J(1), u^j \rangle = \Phi(u^j)$ is equal to 1 if $j = 0$ and is equal to 0 otherwise. This completes the proof of Lemma 7. □

Remark. Most (and in some cases all) of our construction can be carried out for *any* group homomorphism Θ: $Z(q:n) \to Z/(qZ)$. By setting $\Theta = \Phi$, we avoid some generality but substantially simplify some proofs.

IV. Detailed Ring Structure

The algorithms which will be constructed in the second paper require a detailed knowledge of the ring structure of $Z(q:n)$, especially the orbital structure of $Z(q:n)$ under the action of the group $U(q:n)$. For any $0 \le k \le s$, we set $D(k) = p^k U(q:n)$. We call $D(k)$ the orbit of p^k under the action of $U(q:n)$. Since every $a \in Z(q:n)$ can be written as $a = p^k u$ for a unique $k = 0, \ldots s$ and some, not necessary unique, $u \in U(q:n)$, we can write

$$Z(q:n) = \bigcup_{k=0}^{s} D(k) \qquad \text{(disjoint union)}.$$

In the second paper, partial transforms will be taken relative to the sets $D(k)$, $D(j)$, $0 \le j, k < s$.

The sets $D(k)$ can also be described in terms of the ideals of $Z(q:n)$. Observe that $Z(q:n)$ contains the following family of ideals:

$$(0) = (p)^s \subset (p^{s-1}) \subset \cdots \subset Z(q:n)$$

Here $(p^k) = (p)^k$ and (p^k) contains $p^{(s-k)n}$ elements for every k. Then $D(k)$ is the set-theoretic difference $(p)^k \setminus (p)^{k+1}$ implying that $D(k)$ has $p^{(s-k-1)}(p^n - 1)$ elements. Also, $D(0) = U(q:n)$ and for $k > 0$, $D(k)$ contains only zero divisors.

To force uniqueness of our representation of the elements of $D(k)$, we will have to refine our knowledge of the group $U(q:n)$. The ring homomorphism π: $Z(q:n) \to Z(p:n)$ restricts to a group homomorphism, also denoted by π, of $U(q:n)$ onto $U(q:n)$. The kernel H in $U(q:n)$ of π is given by $H = 1 + (p)$. Clearly, H has order $p^{(s-1)n}$. Since $U(p:n)$ is a cyclic group of order $p^n - 1$, $U(q:n)$ contains a cyclic subgroup of order divisible by $p^n - 1$, which is the pre-image $\pi^{-1}(U(p:n))$. Because the order of $U(q:n)$ is $p^{(s-1)n}(p^n - 1)$, $U(q:n)$ contains exactly one subgroup of order $p^n - 1$.

We denote this subgroup by $L = L(s)$ and let x be one of its generators. In the few next lemmas we will explore the structure of $H(s)$.

LEMMA 8. $(1 + (p)^r)^{(p^k)} \subset 1 + (p)^{r+k}$, *for any integer* r *and* k.

Proof. Let us first assume that $k = 1$. Then we have to show that $(1 + (p)^r)^p \subset 1 + (p)^{r+1}$. Indeed, let $a = 1 + p^r b$, for some $b \in Z(q: n)$. Then $(1 + p^r b)^p = 1 + \sum_{j=1}^{p} (p!/(p + j)!j!) p^{rj} b^j$ and the statement follows, since the binomial coefficient corresponding to $j = 1$ is divisible by p. The lemma follows by repeated induction on k. □

LEMMA 9. $(1 + pt)^{(p^{s-2})} = (1 + p^{s-1}t)$, *for any* $t \in Z(q: n)$.

Proof. The proof can be obtained by observing that all the terms of the binomial expansion starting with the third are equal to zero. □

Let $h(i) = 1 + pu^i$, for $i = 0, 1, \ldots, n - 1$. For any i, $h(i)$ is invertible. We will now show that the elements $h(i)$ generate the subgroup H.

LEMMA 10. *The order of* $h(i)$ *is* p^{s-1}.

Proof. The lemma follows immediately from Lemmas 8 and 9. □

LEMMA 11. *The elements* $h(i)$ *satisfy the following "independence" condition*:

$$\prod_{i=0}^{n-1} (h(i))^{a(i)} = 1 \Rightarrow a(i) \text{ is divisible by } p^{s-1} \text{ for every } i.$$

Proof. Let σ be the canonical projection mapping $Z(q: n) \to Z(q: n)/(p^{s-1})$. Observe that the image of σ is isomorphic to $Z(p^{s-1}: n)$. Further, let $h(r, i) = 1 + pu^i \in Z(p^r: n)$, $i = 0, \ldots, n - 1$ for any n. Then $\sigma(h(r + 1, i)) = h(r, i)$. In this new notation, we are going to proof the following statement:

$$\prod_{i=0}^{n-1} (h(r, i))^{a(i)} = 1 \Rightarrow a(i) \text{ is divisible by } p^{r-1} \text{ for every } i. \quad (12)$$

This will be done by an induction on r.

We first assume that $r = 2$. Then

$$\prod_{i=0}^{n-1} (1 + pu^i)^{a(i)} = \prod_{i=0}^{n-1} (1 + pa(i)u^i) = 1 + p \sum_{i=0}^{n-1} a(i)u^i = 1$$

and, therefore, all the coefficients $a(i)$ are divisible by p.

The induction step will proceed as follows. Let $a(i) = b(i) + p^{r-2}c(i)$, for some $b(i)$ and $c(i)$. This presentation is unique. We apply σ to Eq. (12), obtaining

$$1 = \sigma(1) = \sigma\left(\prod_{i=0}^{n-1} (h(r,i))^{b(i)+p^{r-2}c(i)}\right)$$

$$= \sigma\left(\prod_{i=0}^{n-1} (h(r,i))^{b(i)}\right)\sigma\left(\prod_{i=0}^{n-1} \left((h(r,i))^{(p^{r-2})}\right)^{c(i)}\right).$$

Since p^{r-2} is the order of $h(r,i)$, the second term in the last equation is equal to 1. Therefore,

$$1 = \sigma\left(\prod_{i=0}^{n-1} (h(r,i))^{b(i)}\right) = \prod_{i=0}^{n-1} (\sigma(h(r,i)))^{b(i)} = \prod_{i=0}^{n-1} h(r-1,i)^{b(i)}.$$

By induction assumption, $b(i) \equiv 0$ (modulo p^{r-2}). Therefore, we can now reformulate the statement we are proving as follows:

$$\prod_{i=0}^{n-1} (h(r,i))^{c(i)(p^{r-2})} = 1 \Rightarrow c(i) \text{ is divisible by } p \text{ for every } i.$$

By Lemmas 8, 9, and 10 $h(r,i)^{(p^{r-2})} \in 1 + (p)^{r-2}$ and, hence, $h(r,i)^{(p^{r-2})} = (i + p^{r-1}u^i)$. Therefore, we have

$$1 = \prod_{i=0}^{n-1} (1 + p^{r-1}u^i)^{c(i)} = 1 + p^{r-1}\left(\sum_{i=0}^{n-1} c(i)u^i\right).$$

Hence, $c(i) = 0$ and the lemma follows. □

We are now in a position to describe the multiplicative group of the ring $Z(q:n)$.

THEOREM 12. *The group of units of the ring $Z(q:n)$ is isomorphic to the direct sum of the subgroups $H(s)$ and $L(s)$. Further, $H(s)$ is isomorphic to the direct sum of n copies of $Z/(p^{s-1})Z$.*

Proof. We recall that $Z(q:n) = Z(q)[u]/\langle f(u)\rangle$, for some locally irreducible f.

Let us define $H(s,i) = \mathrm{gr}(h(i))$, where gr(...) stands for the subgroup spanned by elements in the parentheses. Lemmas 9 and 11 imply that

$H(s) = \sum_{i=0}^{n-1} H(s,i)$, and the order of $H(s,i)$ is p^{s-1}. Because the latter number is relatively prime to the order of $L(s)$, $U(q:n) \approx L(s) \oplus H(s)$, which completes the proof of Theorem 12. □

EXAMPLES. (1) Let $n = 1$. Then $U(Z(p)) \approx Z/(p-1)Z \oplus Z/(p^{s-1}Z)$ is cyclic of order $p^{s-1}(p-1) = \Phi(q)$, where Φ is Euler's PHI function.

(2) Let $s = 1$. Here $U(p:n) \approx Z/(p^n - 1)Z$, the cyclic group of units of a finite field.

(3) Let $s = 2$. $U(q:n) \approx Z/(p^n - 1)Z \oplus (\sum_{i=0}^{n-1} Z/pZ)$. We observe that $H(2) \approx (Z(p:n))$ and the isomorphism is given explicitly by $t \in Z(p:n) \to 1 + pt$. Here

$$(1 + pt_1)(1 + pt_2) = 1 + p(t_1 + t_2).$$

V. THE ZERO DIVISORS OF $Z(q:n)$

We will now introduce a few more subgroups of $U(q:n)$. Let $H(s,k) = 1 + (p^k) \subset Z(q:n)$.

We observe that $H(s,1) = H(s)$. Further, the subgroups $H(s,k)$ (with $k > 0$ varying) the following sequence is obtained.

$$\{1\} = H(s,s) \subset H(s,s-1) \subset \cdots \subset H(s,1) \subset H(s,0) = Z(q:n). \tag{14}$$

For $k > 0$, $H(s,k)$ is a subgroup of $U(q:n)$.

Remark. Similarly to $H(s)$, $H(s,k)$ is composed of subgroups $H(s,k)(i)$, where $H(s,k)(i) = gr(1 + p^k u^i)$. It is not hard to show that for every i, $H(s,s)(i) \subset H(s,s-1)(i) \subset \cdots \subset H(s,1)(i)$.

The order of $H(s,k)$ is $p^{(s-k)n}$. Hence, the order of the quotient group $H(s,1)/H(s,s-k) = \{1 + (p)\}/\{1 + (p)^{s-k}\}$ is $p^{(s-1)n-(s-s+k)n} = p^{(s-k-1)n}$. Let $L(k) = L(s) \oplus H(s,1)/H(s,s-k)$. The order of $L(k)$ is $(p^n - 1)p^{(s-k-1)n}$.

We are now prepared to examine in greater detail the sets $D(k) = p^k U(q:n)$. Consider the mapping

$$g \to p^k g$$

of $U(q:n)$ onto $D(k)$. This mapping is not one to one. Suppose $p^k g = p^k g'$, $g, g' \in U(q:n)$. Then, $p^k = p^k g' g^{-1}$ which implies that $g'g^{-1} \in 1 + (p^{s-k}) = H(s,s-k)$. Conversely, if $g \in H(s,s-k)$, then $p^k g = p^k$. It follows that the mapping $g \to p^k g$ induces a bijection from the group $U(q:n)/H(s,s-k)$ onto $D(k)$. Set $L(k) = U(q:n)/H(s,s-k)$. Then

the bijection is given by

$$g + H(s, s-k) \to p^k g, \qquad g \in U(q:n).$$

Observe that if $d = p^k g$, $d' = p^k g'$ are any two elements in $D(k)$, then $d' = dg^{-1}g'$. The bijection of $L(k)$ onto $D(k)$ depends upon the representation $D(k) = p^k U(q:n)$. Suppose d_0 is an element in $D(k)$ and is given by $d_0 = p^k g_0$, where $g_0 \in U(q:n)$. Then $p^k = d_0 g_0^{-1}$ and we can write $D(k) = d_0 U(q:n)$. The mapping

$$g \to d_0 g$$

is a mapping of $U(q:n)$ onto $D(k)$. Since $d_0 g = d_0 g'$ implies $p^k g = p^k g'$, we have $gg'^{-1} \in H(s, s-k)$ as before. This implies that the mapping $g \to d_0 g$ also induces a bijection from $L(k)$ onto $D(k)$ given by

$$g + H(s, s-k) \to d_0 g.$$

We summarize this discussion in the following theorem.

THEOREM 13. *Let all notation be as above. For every $d_1, d_2 \in D(k)$ there is one and only one $g \in L(k)$ such that $g^* d_1 = d_2$, i.e., the action of $L(k)$ on $D(k)$ is simply transitive.* □

Remark. In other words, when we consider the action of U on $D(k)$, $H(s, s-k)$ becomes the isotropy group.

COROLLARY. *Every nonzero element of the ring $Z(q:n)$ can be uniquely written as product $p^k x^k h(0)^{k(0)} h(1)^{k(1)} \dots h(n-1)^{k(n-1)}$, where $k = 0, 1, \dots, s-1$, $k = 0, 1, \dots, p^n - 2$, and $k(j) = 0, 1, \dots, p^{s-1} - 1$ for $j = 0, 1, \dots, n-1$.*

Proof. Let $S(k) = \{(k, k(0), k(1), \dots, k(n-1)) | k = 0, 1, \dots, p^n - 2, k(j) = 0, 1, \dots, p^{s-1} - 1 \text{ for } j = 0, 1, \dots, n-1\}$. Let $\mathrm{Exp}(k)$: $S(k) \to Z(q:n)$, $\mathrm{Exp}(k)(k, k(0), \dots, k(n-1)) = x^k h(0)^{k(0)} \dots h(n-1)^{k(n-1)}$. Finally, let $E(k) = \mathrm{Exp}(k)(S(k))$. We observe that

(1) $E(k) \subset D(k)$ (see the definition of $D(k)$).

(2) The number of elements of $S(k)$ is the same as that of $D(k)$.

Thus to prove that $E(k) = D(k)$, we must show that $\mathrm{Exp}(k)$ is a one-to-one function on $S(k)$; this follows from the Theorem 13. To finish the proof, we recall that $Z(q:n) = \bigcup_{k=0}^{s} D(k)$. □

EXAMPLES. (1) Let $n = 1$. We can choose $f(u) = u - 1$. Then $H(s, 1) \approx Z/(p^{s-1})Z$ and so $H(s, 1)$ is cyclic. If we specify $s = p = 3$, we can list

explicitly the algebraic objects discussed above:

$$
\begin{aligned}
(1) &= Z/(27Z) \\
(3) &= \{0,3,6,9,12,15,18,21,24\} \\
(9) &= \{0,9,18\} \\
(27) &= \{0\} \\
D(0) &= U(Z/27Z)) \\
D(1) &= \{3,6,12,15,21,24\} \\
D(2) &= \{9,18\} \\
D(3) &= \{0\}
\end{aligned}
$$

The group of units is cyclic and we can choose 2 as a generator:

$$
\begin{aligned}
U(Z/27Z) &= \{1,2,4,8,16,5,10,20,13,26,25,23,19,11,22,17,7,14\} \\
H(3,1) &= \{1,4,16,10,13,25,19,22,7\} \\
H(3,2) &= \{1,10,19\} \\
H(3,3) &= \{1\} \\
L &= \{1,26\}
\end{aligned}
$$

Here

$(H(3,1)/H(3,2)) \oplus L$ acts on $D(1)$ in the sense of Theorem 13;
$(H(3,1)/H(3,1)) \oplus L \approx L$ acts on $D(2)$.

EXAMPLE (3). Choose $n = 2$, $p = 3$, $s = 2$. The polynomial $f(u) = u^2 + 1$ is locally irreducible over $Z(9)$. The ring $Z(9:2)$ contains 81 elements. Here:

$$
\begin{aligned}
D(0) &= U(9:2) \\
D(1) &= \{3, 3+3u, 6u, 3+6u, 6, 6+6u, 3u, 6+3u\} \\
D(2) &= \{0\} \\
L &= \{1, 2+2u, 8u, 2+7u, 8, 7+7u, u, 7+2u\} \\
H(2,1) &= H(2,1)(0) \oplus H(2,1)(1) = \{1,4,7\} \oplus \{1, 1+3u, 1+6u\} \\
H(2,2) &= \{1\}
\end{aligned}
$$

$(H(2,1)/H(2,1)) \oplus L \approx L$ acts on $D(1)$ in the sense of Theorem 13.

ACKNOWLEDGMENTS

I express my sincere gratitude to Professor L. Auslander, without whose constant encouragement and numerous suggestions this work would undoubtedly never have seen the light of day.

REFERENCES

[AFW] L. AUSLANDER, E. FEIG, AND S. WINOGRAD, "New Algorithms for the Multidimensional Discrete Fourier Transform," IEEE Acoustics.

[AM] M. F. ATIYAH AND I. G. MACDONALD "Introduction to commutative algebra," Addison-Wesley (1969).

[CT] J. W. COOLEY AND J. W. TUKEY, An algorithm for the machine calculation of complex Fourier series," *Math. Comput.* **19**, No. 90 (1965), 297–301.

[R] C. M. RADER, Discrete Fourier transform when the number of data samples is prime, *Proc. IEEE* **5**, **6** (1968), 1107–1108.

[W] S. WINOGRAD, "Arithmetic Complexity of Computations," CBMS-NSF Regional Conference Series in Applied Mathematics, 1980.